Amendments to the Claims:

Please cancel claims 1-28. Please add new claims 29-42 as indicated. This listing of claims will replace all prior versions, and listings, of claims in the application. No new matter is presented.

1-28. (Cancelled)

29. (New) A system for mutually authenticating a client operatively coupled to a communications network to a device operatively coupled to the communications network, the communications network comprising the client and the device, the device operatively coupled to a key database, the key database comprising client keys stored in association with unique client identifiers, the system comprising:

a client physical token adapted to be operatively coupled to the client, the client physical token comprising a client random number generator, a unique client identifier, and a client key;

a device physical token adapted to be operatively coupled to the device, the device physical token comprising a device random number generator;

client software adapted to be installed on the client to send a first challenge to the device, the first challenge comprising a first random number generated by the client random number generator and encrypted using the client key, the first challenge further comprising the unique client identifier; and

device software adapted to be installed on the device to retrieve a stored client key associated with the client identification in the first challenge and decrypt the first random number in the first challenge using the retrieved client key, whereby decrypting the first random number authenticates the client computer to the device;

wherein the device software, when installed in the device, sends a second challenge to the client, the second challenge comprising a second random number different from the first random number and generated by the device random number generator and encrypted using the client key;

wherein the client software, when installed in the client, decrypts the second random number using the client key, whereby decrypting the second random number authenticates the access point to the client computer;

wherein subsequent data sent between the device and the client is encrypted using a key derived from the first random number and the second random number.

30. (New) The system of claim 29 in which the device is a wireless access point.

31. (New) The system of claim 29 wherein the client physical token is removable from client.

32. (New) The system of claim 31 wherein the client physical token is removable from client by a user.

33. (New) The system of claim 29 wherein the device physical token is removable from the device.

34. (New) The system of claim 33 wherein the device physical token is removable from the device by a user.

35. (New) The system of claim 29 wherein no key is exchanged between the device and the client during authentication.

36. (New) A method of mutually authenticating a client operatively coupled to a communications network to a device operatively coupled to the communications network, the communications network comprising the client and the device, the device operatively coupled to a key database, the key database comprising client keys stored in association with unique client identifiers, the method comprising:

providing a client physical token adapted to be operatively coupled to the client, the client physical token comprising a client random number generator, a unique client identifier, and a client key;

providing a device physical token adapted to be operatively coupled to the device, the device physical token comprising a device random number generator;

providing client software adapted to be installed on the client to send a first challenge to the device, the first challenge comprising a first random number generated by the client random number generator and encrypted using the client key, the first challenge further comprising the unique client identifier; and

providing device software adapted to be installed on the device to retrieve a stored client key associated with the client identification in the first challenge and decrypt the first random number in the first challenge using the retrieved client key, whereby decrypting the first random number authenticates the client computer to the device;

wherein the device software, when installed in the device, sends a second challenge to the client, the second challenge comprising a second random number different from the first random number and generated by the device random number generator and encrypted using the client key;

wherein the client software, when installed in the client, decrypts the second random number using the client key, whereby decrypting the second random number authenticates the access point to the client computer;

wherein subsequent data sent between the device and the client is encrypted using a key derived from the first random number and the second random number.

37. (New) The method of claim 36 in which the device is a wireless access point.

38. (New) The method of claim 36 wherein the client physical token is removable from client.

39. (New) The method of claim 38 wherein the client physical token is removable from client by a user.

40. (New) The method of claim 36 wherein the device physical token is removable from the device.

41. (New) The method of claim 40 wherein the device physical token is removable from the device by a user.

42. (New) The method of claim 36 wherein no key is exchanged between the device and the client during authentication.